GLOBAL LEDGER

# Nobitex's Longstanding Fund Obfuscation Tactics Revealed

Investigation

# Executive Summary

Following the June 18, 2025 hack on Nobitex that resulted in the loss of approximately $90 million, blockchain analysis shows that **a significant portion of the exchange's reserves remain intact** and are being actively managed.

Just hours after the breach, Nobitex transferred **1,801 BTC** (**worth about $187 million**) from its exposed wallets to newly created addresses. These transfers were followed by further movements into a **rescue wallet**, and later to a new destination holding **1,783 BTC**, suggesting **continued operational control** over large amounts of liquidity.

While Nobitex's past wallet behavior raises concerns due to repeated use of peelchain-like structures, the current flows confirm that **the platform retains substantial reserves post-hack**.

# Background

**On June 18, 2025**, the Iranian crypto exchange **Nobitex** was compromised in a coordinated attack affecting multiple blockchains. Approximately **$90 million** worth of assets were drained across eight networks and sent to burn addresses, removing them from circulation unless stablecoin issuers decide to intervene and remint the lost value. The pro-Israeli group **Gonjeshke Darande** later claimed responsibility.

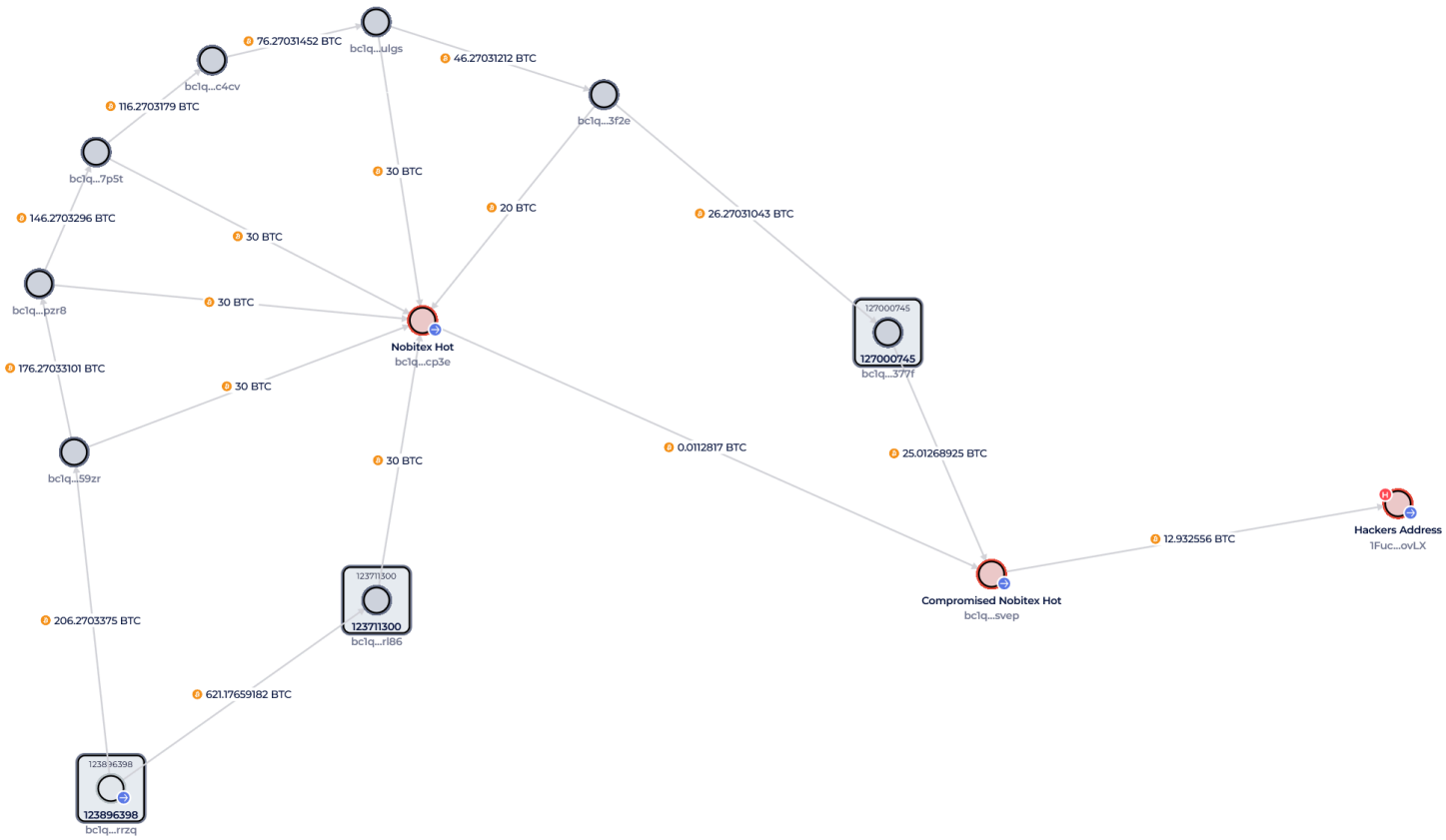
In the aftermath, what began as a breach investigation quickly revealed something more troubling. As we examined Nobitex's on-chain infrastructure, it became clear the real story wasn't just about the attackers, but about the internal patterns and behaviours that had been quietly unfolding for months.

# Analysis Findings

While reviewing wallets linked to **Gonjeshke Darande**, one Bitcoin address stood out: **1FuckiRGCTerroristsNoBiTEXXXaAovLX**. Tracing its activity revealed that Nobitex appeared to be engaging in what looked like laundering operations involving several of its own hot wallets.

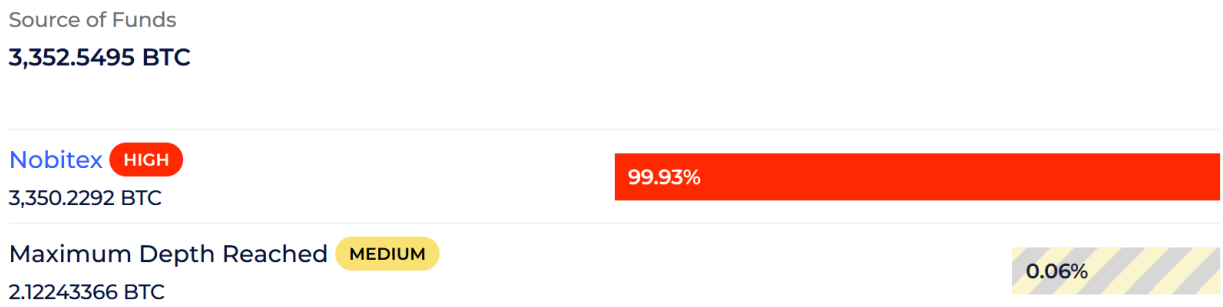
It became clear that Nobitex had previously relied on temporary one-use deposit and withdrawal addresses. This method is known in the cybersecurity world as a **chip-off or peelchain technique**. It involves gradually splitting large sums into smaller amounts and passing the “change” to the next address until the money trail becomes unreadable. The purpose is to quietly cash out funds without drawing attention.

Tracing this activity backwards we came across a wallet **bc1q...rrzq** where the suspiciously-looking fund flow originated from.



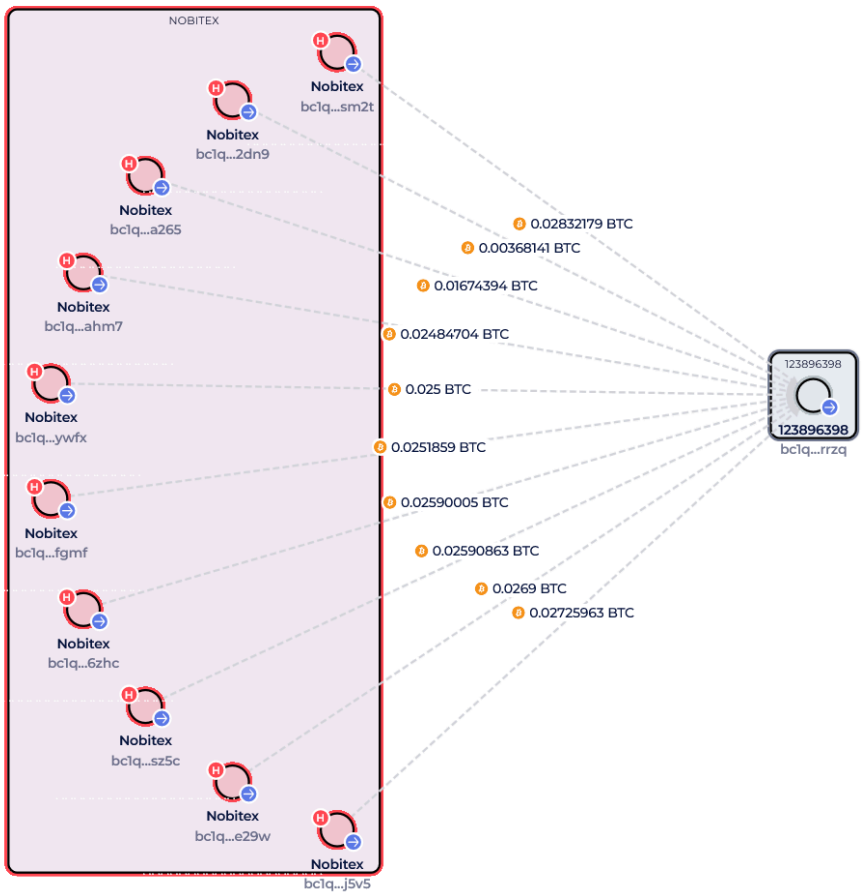

**Pic 1. Chipping-off funds originating from a suspicious wallet to two Nobitex hot wallets over time**

To determine ownership, we performed a counterparty analysis of **bc1q...rrzq**, identifying all wallets that had ever sent funds to it.




**Pic 2. Counterparty report on a wallet bc1q...rrzq where the laundering-like behaviour originated from.**

As shown, virtually all funds originate from wallets associated with Nobitex. Beyond that, this wallet's on-chain behavior aligns with typical centralized exchange activity — namely, multiple user wallets consolidating funds into a single address.

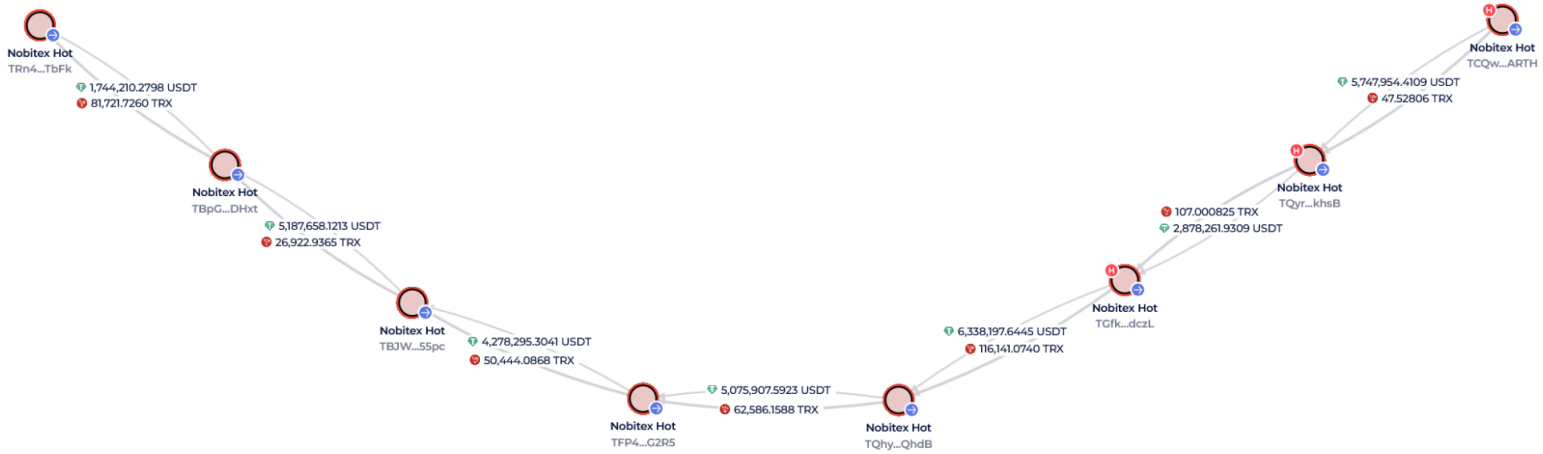



**Pic 3. Nobitex users' deposits to a wallet bc1q...rrzq where the laundering-like behaviour originated from. — PIC**

Another common technique, particularly across centralized exchanges, is the internal transfer of liquidity between operational wallets, each with a limited service “lifespan”.

As we will see on Pic. 1, on March 16th Nobitex’s hot wallet **bc1q...cp3e** passed its remaining liquidity of **0.01128170 BTC** to the compromised hot wallet.

The same behavioral pattern is seen on other chains (**Tron in this case**) where Nobinex is operating. On this graph we see a number of hot wallets passing liquidity between each other over just 3 months.



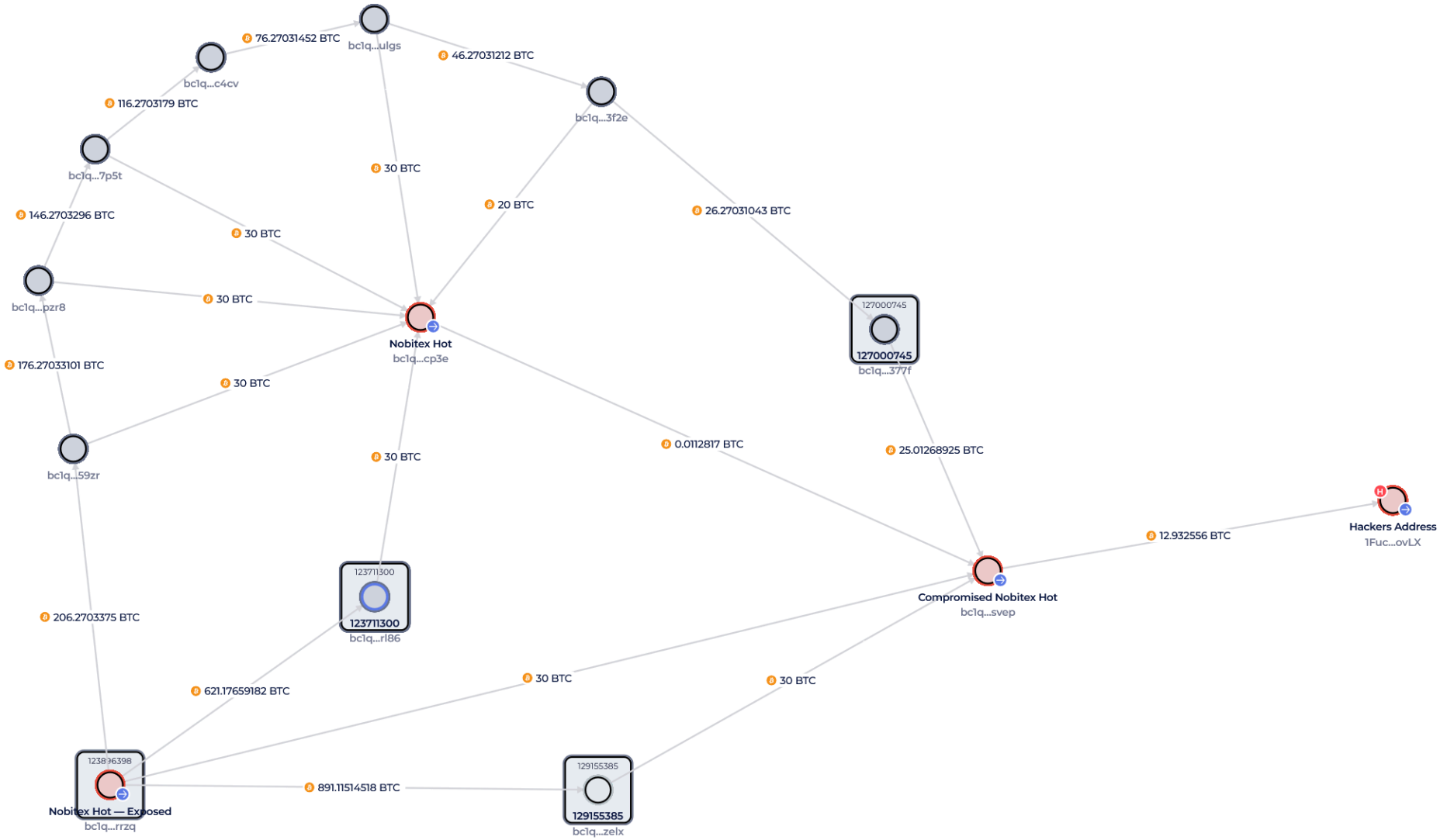

**Pic 4. Liquidity transfer between Nobitex hot wallets in TRON network within 3 months period**

All this collective evidence gave us an undeniable proof as to its attribution as a **Nobitex hot wallet**.

---

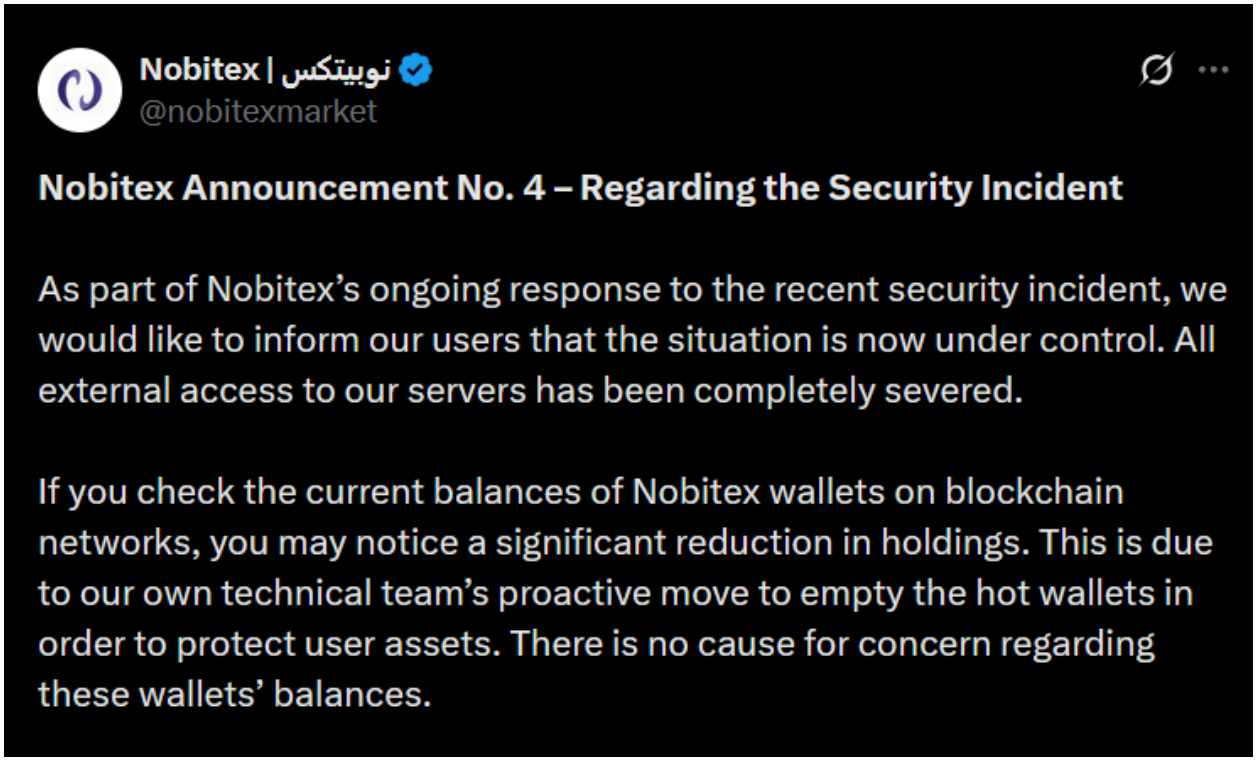
As the analysis continued, it became evident that **three hot wallets belonging to Nobitex**, including the one compromised in the attack, had been involved in similar peelchain activities.

These wallets consistently passed significant amounts of BTC, often **30 BTC per transaction**, between intermediary addresses in ways that suggested an effort to **obscure fund flows**.




**Pic 5. Chipping-off funds originating from Nobitex's exposed hot wallet to two other Nobitex hot wallets over time.**

Shortly after the hack, Nobitex released a statement claiming that, as a safety measure, **liquidity was moved from its hot wallets** those that had not been drained during the attack.



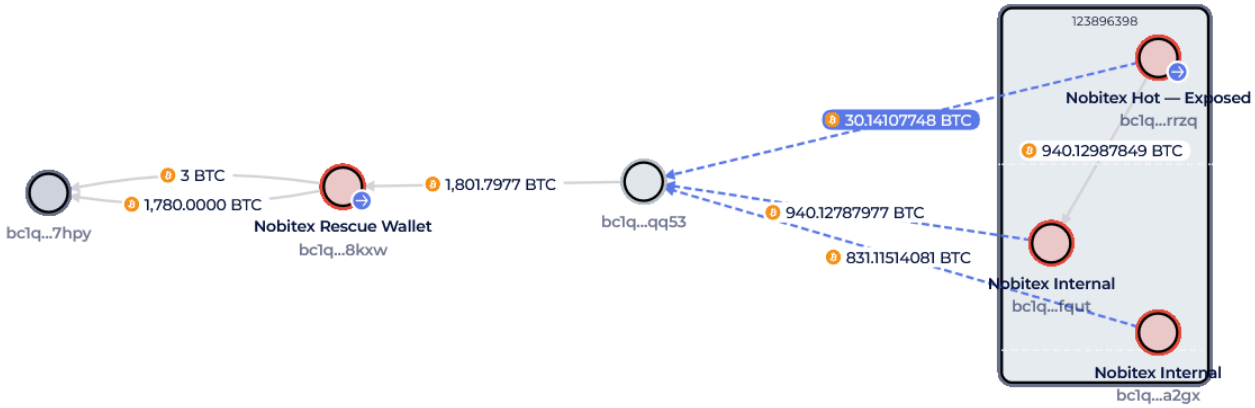

This aligns with the on-chain activity we observed next, involving Nobitex's exposed hot wallet.

## Sudden Fund Movements

Roughly **eight hours after the hack** that happened at **05:02:45 UTC** on the Bitcoin network, Nobitex's exposed hot wallet and a few other internal wallets (which were all previously taking part in peelchain activity) performed a major transaction at **13:22:21 UTC**. **It emptied out all of its balances**, moving the funds into a newly created wallet **bc1q...qq53**. This kind of full sweep is commonly used to transfer all assets under control of a single owner into a new address.

The sweep involved **1,801.7981 BTC**, equal to about **$187.5 million**. The funds were first moved to **bc1q...qq53**, and then sent again to what is believed to be Nobitex's rescue wallet.

Later, on **June 19 at 11:29:15 UTC**, **1,780 BTC** were moved again to a newly created wallet **bc1q...7hpy**, followed by a smaller transfer of 3 BTC.

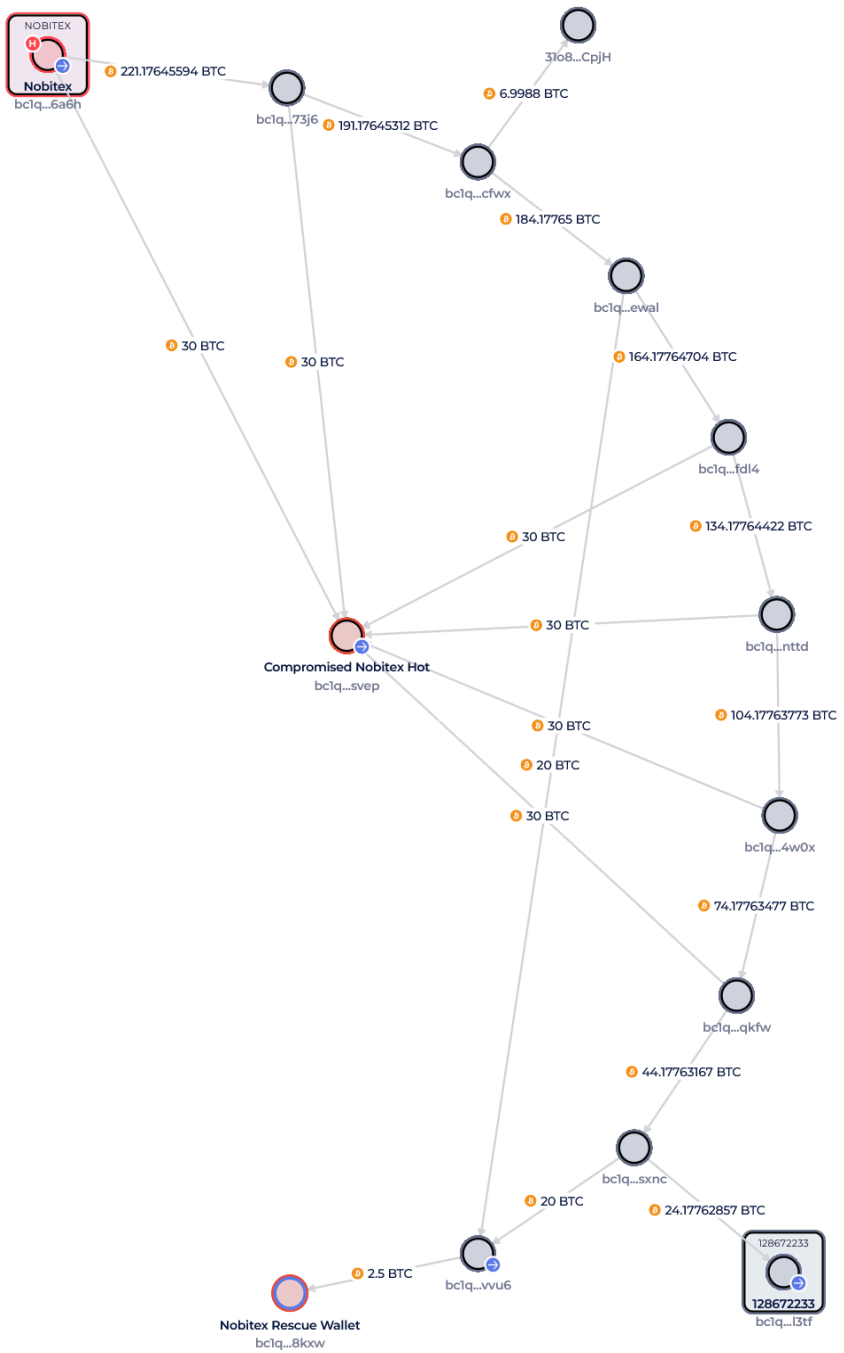



**Pic. 6 Sweep transaction with further liquidity move (left) along with chip-off to compromised Nobitex hot wallet (right)**

## Nobitex Rescue Wallet

Nobitex's rescue wallet appears to have been acting as a consolidation address historically, **regularly receiving chipped-off amounts** since October 2024. The funds were then **peelchained**, eventually ending up on exchanges or other services or even sent directly to known wallets connected to illicit actors. Once again, we see multiple **30 BTC transfers** to the compromised Nobitex wallet followed by a peel-chain leading to the rescue wallet.

As we can see, funds are originating from the Nobitrex cluster following a series of intermediary wallets chipping off typical chunks of 30 or 20 BTC as the peelchain progresses.

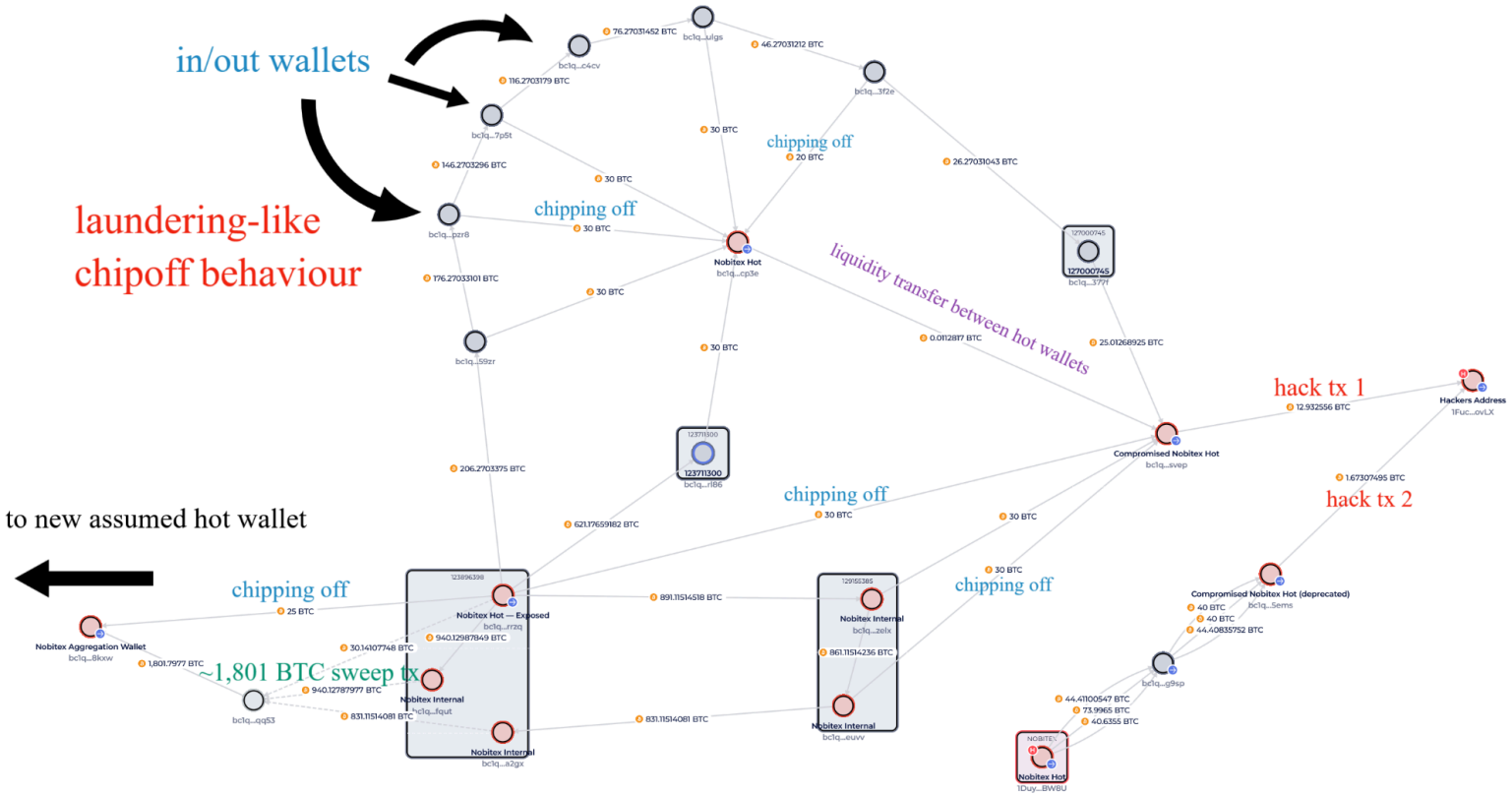



**Pic. 6 Historical demonstration of chip-off patterns involving the compromised Nobitex hot wallet and the rescue wallet**

## The Bigger Picture

On the following general scheme we see several examples of chip-off laundering behaviour involving both entities. In the middle you can find an **older Nobitex** hot wallet which at the end of its operational activity passed the remaining liquidity to a new hot wallet (the compromised one) in its final transaction.

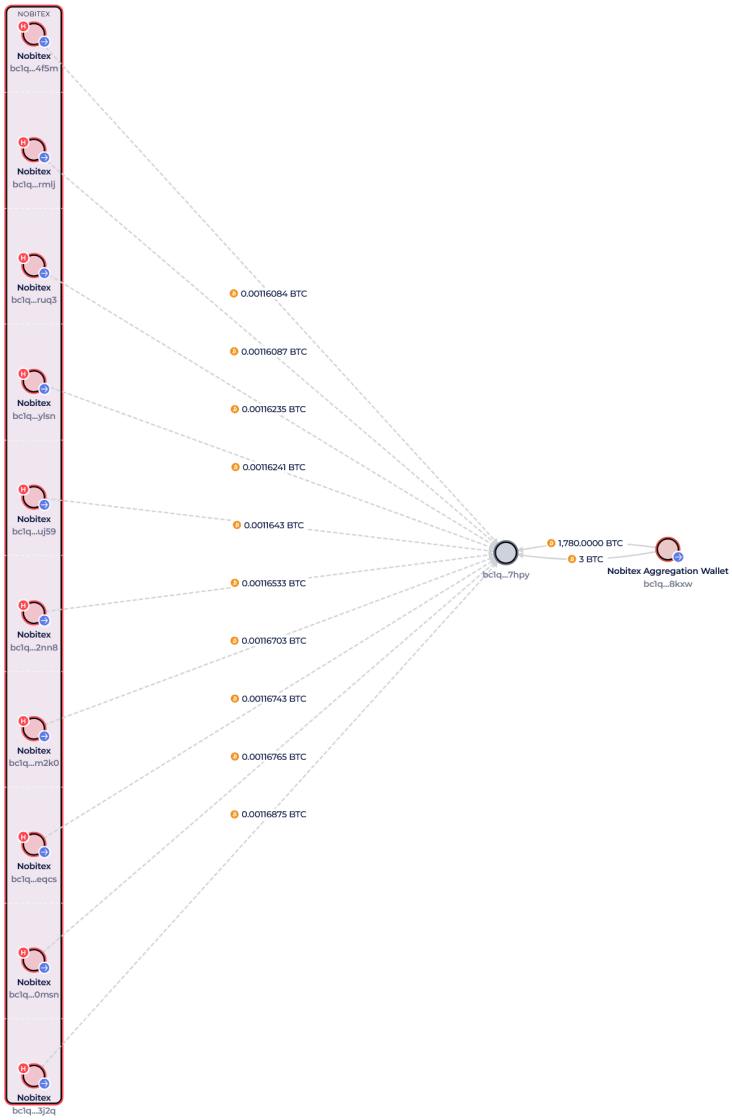
Another transaction in the scheme originates from the second compromised Nobitex wallet that had not been used since March 2021.




**Pic. 7 General picture of the hack transactions and the Nobitex's peelchain activity**

On **June 19 at 07:00 UTC**, Gonjeshke Darande published documents linked to the hack, casting doubt on Nobitex's earlier statements about fund recovery.

Then on **June 20 at 02:12:52 UTC**, a wave of inbound transfers from the Nobitex cluster was observed reaching a wallet holding **1,783 BTC** previously received funds (and what is assumed to be a liquidity transfer from the exposed Nobitex wallet). This perfectly correlates to a previous statement by Nobitex assuring its users that the platform is taking remedial actions moving liquidity to a new hot wallet.




**Pic. 8 Nobitex users funds move to what is believed to be a new hot wallet**

# Conclusions

While investigating the Nobitex hack, we uncovered something more than just a theft. The on-chain behavior points to a long-running pattern of suspicious fund movements not only during the breach, but well before it.

Techniques often associated with money laundering, such as peelchains, usage of one-time intermediary wallets, frequent liquidity transfers, and sweeping entire balances, were already in place within Nobitex’s infrastructure. These weren’t isolated reactions to the hack, but signs of how the exchange may have been operating under the radar for months.

After the breach, Nobitex described its fund movements as safety measures but the scale and timing suggest a deeper story. What looked like damage control also resembled long-practiced liquidity concealment.

This doesn't change the fact that Nobitex was attacked. But it does raise uncomfortable questions about what was happening behind the scenes and whether the hack merely brought longstanding issues to the surface.

In the end, the breach didn’t just drain assets - it pulled back the curtain.